FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING FATF



1998-1999 REPORT ON MONEY LAUNDERING TYPOLOGIES

All rights reserved. Applications for permission to reproduce all or part of this publication should be made to: FATF Secretariat, OECD, 2 rue André Pascal, 75775 Paris Cedex 16, France

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING 1998-1999 REPORT ON MONEY LAUNDERING TYPOLOGIES

I. INTRODUCTION

- 1. The group of experts met on 17-18 November 1998 under the chairmanship of Mr. Simon Goddard, Head of Intelligence, Strategic and Specialist Intelligence Branch, National Criminal Intelligence Service (NCIS). The meeting took place in the conference room of the European Bank for Reconstruction and Development (EBRD) in London. The group comprised representatives of the following FATF members: Australia, Austria, Belgium, Canada, Denmark, European Commission, Finland, France, Germany, Ireland, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Experts from non-member international organisations with observer status, namely the Council of Europe, Interpol, the International Organisation of Securities Commissions (IOSCO), and the World Customs Organisation (WCO), also attended the meeting. The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (PC-R-EV) was represented by Slovenia.
- 2. The purpose of the 1998-1999 typologies exercise was, as in previous years, to provide a forum for law enforcement and regulatory experts to discuss recent trends in the laundering of criminal proceeds, emerging threats, and effective countermeasures. While discussions of this exercise generally focus on money laundering developments within FATF member nations, the experts also attempt to examine available information on current money laundering patterns in non-member countries and other regions of the world. Prior to the meeting, delegations were invited to provide written submissions to serve as the starting point for discussions. In a departure from the format of earlier typologies exercises, this year's meeting was led off with in-depth presentations on a series of major money laundering issues that had been agreed upon during the FATF plenary meeting in September 1998.
- 3. The present report, therefore, focuses first of all on these major issues: the euro currency unit and large denomination banknotes, problems associated with offshore financial centres of non-cooperative countries or jurisdictions, challenges posed by new payment technologies, and the potential use of the gold market in money laundering operations. The report then continues with an examination of other money laundering trends in FATF countries followed by the overview of trends in non-member jurisdictions.

II. MAJOR MONEY LAUNDERING ISSUES

(i) The single European currency and large denomination banknotes

4. The euro currency unit became the single currency of eleven European Union member states¹ on 1 January 1999. At that time, existing national currencies of the participating members became simply an expression of the euro. During the 'transitional' period that started on 1 January, the euro will not be issued in physical form; the participating members will continue to use their existing coins and notes. On 1 January 2002, euro coins and banknotes will be introduced, and, the existing national currencies of the participating members will then be withdrawn as legal currency by 30 June 2002 at the latest. The exact

¹ The eleven EU members involved in the introduction of the new currency include: Austria, Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Portugal, and Spain.

time for this final 'changeover' period (to occur between 1 January and 30 June 2002) will vary according to the implementing legislation of the individual participating member states.

a. Impact on Money Laundering

- 5. The primary period of potential risk is the six-month window during which the national currencies in paper and coin form will be exchanged for the euro. Some experts expressed the fear that money launderers might use this window to try to introduce illegally derived funds by hiding them among the expected higher volume of operations involving 'exchanges' of national currency for the euro. Other experts believed that there might be a rise in laundering in the time before the changeover by using traditional methods, by exchanging these funds for currency from outside the euro zone, or by increased use of professional services providers all to avoid detection during the actual changeover period.
- 6. With the elimination of 11 national currencies, it was agreed that the role of bureaux de change in the countries of the euro zone would diminish with regard to money laundering and its detection. Nevertheless, there could be an increase in exchange activities in those European countries outside the euro zone, especially involving traditional currencies such as US dollars, UK pounds, and Swiss francs. Moreover, once money has been converted to euros, the movement of these funds over national borders within the countries of the euro zone will cause less notice. One northern European country stated in its written submission that it might see an overall increase in the volume of cash in circulation prior to 1 January 2002 (with, for example, a possible influx of non-EU money specifically Russian held US dollars exchanged for euros).
- 7. The experts believed that there was little likelihood that international money launderers would convert national currencies to the currencies of non-participating countries (Danish or Swedish kroner, Greek drachma). The only exception, as mentioned above, is the UK pound, which will likely continue to be important in laundering related to certain types of narcotics activity. As for FATF countries in other areas of the world, the experts were of the opinion that the changeover to the euro would have little affect on laundering in North America, Asia or Australia, where the US dollar will probably continue to be the primary currency used in such activity. They recognised, however, that the euro used in wire or electronic transactions may turn up in money laundering operations anywhere in the world after 1 January 1999.

b. Impact on Anti-Money Laundering Measures

- 8. Almost all of the FATF member countries who are taking part in the changeover to the euro have started to pay attention to the specific money laundering concerns surrounding the introduction of the euro. The Netherlands, for example, has had a working group since 1996 to examine the problem and provide recommendations on necessary countermeasures. In Germany, the Federal Criminal Police produced a study in early 1998, which addresses the issue of the euro introduction as related to potential criminal activity. Italy has also set up a euro implementation co-ordinating committee of relevant ministries and authorities that will issue detailed implementation rules that take in to account the money laundering risks.
- 9. Many delegations felt that current anti-money laundering (preventive) systems should be adequate for detecting potential money laundering in this area. Since the changeover to the euro in banknote and coin form will require that national currency be physically presented at a financial institution, there was also felt to be a greater risk of detection for the launderer involved in such cash transactions. It was stressed that all member countries should continue to promote vigilance at financial institutions with regard to suspicious transaction reporting both prior to and during the changeover period.

- 10. The experts considered the possibility that the increased volume of all activity during the changeover period might overwhelm financial institutions personnel and might make them therefore more likely to miss or disregard potential indicators of money laundering. Another concern was related to which institutions actually perform the currency conversions. One FATF member country feared that non-bank financial institutions involved in the changeover might not have adequate guidance on what constitutes suspicious activity regarding euro conversions.
- 11. A number of FATF members mentioned that they would increase awareness of the issue and reinforce anti-money laundering measures during the transition period. In the Netherlands, the potential problem with non-bank financial institutions is being dealt with by permitting only banks to carry out exchanges of national currency for euros. Germany will permit other financial services to perform these exchanges, however, only when these institutions are licensed to do so by the Federal Banking Supervisory Office (as is also required for operating a retail foreign exchange business). Additionally, the Federal Banking Supervisory Office issued new guidelines in March 1998 that lowers the threshold (whereby customer identification is required) to DEM 5,000 (USD 3,018) for conversion transactions.
- 12. Other issues brought up by the experts related to cross-border implications of the introduction of the euro both within and outside the countries of the euro zone. Italy mentioned that conversions of large amounts of national currency in other than its country of origin should be an indicator of suspicious activity. Similarly, conversions of large amounts of national currency to euros by individuals domiciled in other countries might also be a suspicious indicator. The United States raised the question of how existing national currencies (of the euro zone countries) held abroad will be exchanged for euros. These concerns highlight the fact that an internationally co-ordinated approach relative to the introduction of the euro still must be articulated for developing common money laundering indicators, specific sector guidelines, and sharing the information procedures among relevant national anti-money laundering services.
 - c. Introduction of the Large Denomination Euro Banknote
- 13. With the introduction of the euro in banknote and coin form (after 1 January 2002), the highest denomination banknotes will be EUR 500. This note will be roughly comparable in value to the highest denomination banknotes issued by Germany and the Netherlands. A number of FATF members have expressed concern that the issue of the high denomination euro banknote might make the currency more attractive to money launderers.
- 14. Several of the delegations saw the introduction of the large denomination euro as not only relating to the euro currency but also a potential problem in all countries having high denomination banknotes. Some of the countries of the euro zone already have high denomination notes (Austria, Belgium, Germany, the Netherlands), and the EUR 500 note was designed, according to the European Commission, to fulfil a similar role to that of the original national currency. Moreover, there are large denomination banknotes in other FATF member countries as well (Canada, Singapore, Switzerland), which may continue to exist after the introduction of the euro.
- 15. The legal use of large denomination notes is currently may often be concentrated in certain economic sectors (used automobiles, livestock, etc.) although this use could not account for all of the large denomination notes issued. Most delegations, including those from countries with large denomination banknotes, recognised that incomplete information is available on the legitimate use of these notes.
- 16. A number of FATF member countries have observed that large denomination notes tend to be used in the hoarding of money related to tax evasion or avoidance and in criminal activity. US cases illustrated

how the bulk of small denomination currency and the difficulties involved in transporting it are still the primary obstacle for money launderers (and one of the easiest ways to detect them). As a further example of criminals preferring large denomination notes, Germany stated that kidnappers routinely demand that ransom money be provided in DEM 1,000 notes. In Canada, the CAD 1,000 bill was originally introduced to facilitate bank to bank transfers. This licit use has become outmoded with the ability of banks to transfer funds more rapidly and safely by electronic means. Criminal money movements with these banknotes now show up almost exclusively as related to casino winnings. A case was cited in which CAD 70 million (nearly USD 45.7 million) in CAD 1,000 bills were alleged to have transited or still to be located in safety deposit boxes of a bank in central Europe.

- 17. Despite the fact that there is an incomplete understanding of the uses of large denomination banknotes in the legitimate economy, some of the experts felt strongly that the introduction of the EUR 500 banknote after 1 January 2002 may facilitate laundering. Other experts believed that large denominations may only facilitate movement of cash (whether legitimate or not) and not money laundering. Large denomination banknotes draw too much attention at financial institutions, thus presenting a potential launderer with increased risk of detection; therefore, 'middle-sized' denominations might be more suitable for the purpose of money laundering. Criminal proceeds denominated in EUR 500 banknotes would be considerably less bulky than the equivalent value of funds denominated in USD 100 bills. Current antimoney laundering measures within FATF members should be adequate for detecting suspicious cash transactions (including large denomination banknotes). However, with the expanded geographic region that comprises the euro area, there will be fewer internal points at which to detect suspicious currency shipments. It was therefore suggested that study of the subject should continue with a view toward clarifying the legal and illegal uses of large denominations.
- 18. In discussing the use of large denomination banknotes for laundering, and in particular the potential use of the EUR 500 note after 1 January 2002, the experts drew attention to the fact that the money laundering implications of the EUR 500 note do not appear to have been considered in planning for this large denomination banknote. The reason that the EUR 500 banknote was developed was to offer a denomination that would correspond with already existing high denomination banknotes in the countries of the euro zone. It was also noted by some of the experts that the use of high denomination notes in potential illegal activities, such as money laundering or tax evasion, was not taken into account. One delegation indicated that this issue had indeed been considered. Although experts mentioned a few economic activities in which the use of large denomination banknotes is especially common, the role of these denominations in legitimate commerce has apparently not been examined either. The majority of the FATF experts considered that the potential legitimate and illicit uses of large denomination banknotes ought to be thoroughly examined by the European Central Bank Furthermore, a number of the experts called for the FATF member countries to continue to study the subject with a view toward augmenting any other examination at the international level.

(ii) Offshore financial centres of non-cooperative countries or territories

19. During the past ten years, FATF member countries have made significant progress in adopting anti-money laundering regimes based on the standards set forth in the FATF Forty Recommendations. This progress has also been reflected in the increasing co-operation among members on anti-money laundering investigations. In non-member countries and jurisdictions, there have been signs more recently of an increased willingness to follow the FATF Forty Recommendations and co-operate on anti-money

laundering investigations. This increased acceptance of FATF standards contrasts, however, with the unwillingness or outright refusal of certain important financial centres to co-operate in this area. The issue of non-cooperation was therefore identified by FATF members as one that should be addressed during the annual typologies exercise. The typologies discussions on the subject would then serve as a starting point for broader discussions on the issues of international co-operation. Prior to the experts meeting, FATF members were asked to examine the specific operational problems or difficulties that they had encountered with offshore financial centres in such areas as banking secrecy, shell companies, identification of beneficial owners, exchange of information, and other forms of international co-operation.

a. Impact on money laundering

- 20. Past typologies exercises began the task of identifying how 'offshore financial centres' facilitate money laundering. The experts at this meeting agreed that schemes involving these jurisdictions still appear to share common characteristics: a series of multiple financial transactions through the centre, use of nominees or other middlemen to manage these transactions, and an international network of shell companies (including a specialised 'off-the-shelf' variety that immediately go dormant upon completion of the series of transactions). Often an individual money laundering scheme will include more than one of these centres. An investigating agency can usually see the path that questionable funds follow into or out of such a scheme; however, the exact links between the funds and the illegal act that generated them are lost. Investigations of this type are often therefore unable to be fully exploited to a successful conviction or confiscation.
- 21. The oft-stated reason for creating an offshore financial centre has been to provide certain fiscal advantages to natural or legal persons that use its services. Since tax evasion schemes and money laundering operations often appear to use similar techniques, many money laundering experts believe that the quest for optimal 'fiscal advantages' is frequently used as a cover for moving to or through such locations what are in reality criminally derived moneys. One expert pointed out during this exercise, however, that there appears to be one significant difference between the techniques used for taking fiscal advantage of an offshore location and laundering criminal funds. In the former case, the funds usually move to a single offshore location where they are sheltered from the home country's fiscal oversight. In the latter case, that is, involving criminally generated funds, the tendency is for the funds to move rapidly through several offshore locations.
 - b. Impact on anti-money laundering measures: Role of the foreign legal entity
- 22. Virtually every FATF member represented at the experts meeting reported having experienced problems in pursuing anti-money laundering investigations with links to offshore financial centres. However, it was also pointed out that some offshore centres of non-cooperative countries were attempting to improve the level of judicial or investigative co-operation within the current framework of their national laws or by making selected changes to their legislation. The experts agreed, therefore, that the problem was most acute with those jurisdictions that are slow or unwilling to assist in international anti-money laundering investigations, particularly in regard to identifying the beneficial owners of legal entities.
- 23. FATF written submissions and a certain amount of discussion by the experts focused on the major problem posed by foreign legal entities to successful conduct of anti-money laundering investigations. Obtaining information from some offshore jurisdictions on the true owners or beneficiaries of foreign registered business entities shell companies, international business companies, offshore trusts, etc. appears to be the primary obstacle in investigating transnational laundering activity.

- 24. A number of FATF member countries mentioned that they regularly attempt to request information on foreign legal entities using mutual legal assistance treaties or other agreements with the offshore jurisdiction. Often non-cooperative jurisdictions refuse to respond to a foreign request for investigative or judicial assistance because there is no bilateral agreement that would permit such co-operation. The jurisdictions might also refuse the foreign request because the information requested is not maintained in any official registry. In some cases, information on legal entities may be protected from disclosure to foreign investigative agencies because of strict banking secrecy (with a variation related to non-release of fiscal information, including criminal or civil liability for disclosure) that is impenetrable even to domestic judicial or regulatory authorities. Some delegations also mentioned the increasing use of the Internet for the marketing and provision of such services.
- 25. The experts also highlighted the role of professional services providers in ensuring the good functioning of money laundering operations through non-cooperative jurisdictions. These solicitors, accountants, financial consultants, and company formation agents facilitate the creation of appropriate business entities that serve as the pipeline for moving funds of legal, as well as illegal, origin. Typically, such services are provided to non-residents of the jurisdiction and often at a higher level of confidentiality than that available to residents.

c. Potential solutions

26. In this regard, the experts hoped that the FATF ad hoc group on non-cooperative countries and territories, which was established in September 1998, would be able to develop strategies for addressing the issue. Several members pointed out that they are able to rely, in some cases, on existing international mechanisms for the exchange of information relating to money laundering investigations: mutual legal assistance treaties, memoranda of understanding, and Interpol. Nevertheless, these mechanisms do not work when the jurisdiction receiving the request for assistance refuses to honour it or does not maintain the desired information. The consensus of the experts was that every country or jurisdiction should have a mechanism in place for establishing the beneficial owners of legal entities registered within it and should have the authority to share this information with foreign counterpart investigative agencies. The development of internationally recognised minimum registration requirements would be welcome in this regard. Some of the written submissions also suggested that the so-called 'fiscal exemption' should no longer be valid grounds for refusing a foreign request. The work of the Egmont Group of Financial Intelligence Units (FIUs) was also mentioned as a potential channel for resolving this issue, given its work at the operational level to facilitate information sharing and the fact that many offshore financial centres already take part in its activities.

(iii) New payment technologies

- 27. All delegations continue to report that there have not been as of yet any investigated money laundering cases involving the new payment technologies identified in previous typologies reports. However, there have been several instances of other types of crimes generally fraud schemes against unsuspecting members of the public that have used the Internet as a means for committing the underlying offence. Law enforcement in FATF member countries remains concerned about the potential for use of these new technologies in money laundering schemes. Specifically, some of these risks include:
- inability to identify and authenticate parties that use the new technologies;

- level of transparency of the transaction;
- lack or inadequacy of audit trails, record keeping, or suspicious transaction reporting by the technology provider;
- use of higher levels of encryption (thus blocking out law enforcement access); and
- transactions that fall outside current legislative or regulatory definition.
 - a. Status of new payment technology systems
 - (1) Smartcards
- 28. Smartcards or electronic purses have been developed as an alternative to currency in paper and coin form. The electronic chip in the card can then store monetary value in electronic form which may then be spent as currency. Because the value on the card has already been debited from the financial institution, if the card is lost, there is no loss to the institution. There is thus no inherent reason for the financial institution to restrict the amount that may be held on an individual card
- 29. Smartcard systems in FATF member countries are mostly still in the prototype or early testing phases. Among these systems, there are many variants in terms of specific operating characteristics. Some of the systems are designed to provide transactional anonymity, while others capture data which may be used to construct an audit trail. In this regard, FATF members expressed some concern over the development of smartcard distribution through automated vending machines, which would allow virtually anonymous transfer of value to these cards. Within FATF member countries, the issuers/operators of many smartcard systems have placed limits on the amount of money that may be loaded onto the cards (for example, UK institutions have set the limits at GBP 50 500 [USD 82 820]); however, it was noted that this is not always the case. In one example, an institution in a non-FATF member country reportedly markets a smartcard with an upper limit of USD 92,000. Furthermore, while most smartcard systems do not permit so-called 'peer-to-peer' (direct 'card-to-card') transactions, others are developing the capability to move funds among card holders without recourse to a financial intermediary. In any case, it should be noted that, where there are limitations on card functions, these have been set by the card issuers and not by the respective national regulatory authorities.

(2) *On-line Banking*

- 30. On-line banking has increasingly come to mean the method whereby certain types of financial transactions may be performed through the Internet website of those banks that offer this service. FATF members reported that there is a great deal of growth in this area. In the United States, nearly 85% of financial institutions have or are planning to establish such services. A significant number of financial institutions in other countries have also set up on-line facilities. In its most basic form, the service provided includes verification of cheque account balances and transfers among accounts at the same institution. In those systems that allow payments or transfers to be made, the customer is often restricted in the amount of transaction or the identity of the beneficiary. All of the systems require that on-line operations be tied to an already existing account at the institution; therefore, there is a continuous record of account activity.
- 31. The concerns mentioned in this area refer, again, primarily a lack of uniform regulation from supervisory authorities. Thus, although the customer's activity is tied to a particular account set up in his name, there is no way to verify the identity of the Internet transactor once the account has been opened. Indeed, if the on-line financial institution is located in an area known for high levels of banking secrecy and requires little or no proof of identity for opening an account, the money launderer could theoretically move

funds from the convenience of his computer terminal. Although there were no reported cases of this type of laundering taking place at this time, the experts believed that technology was developing rapidly and thus worthy of further vigilance.

(3) *E-Cash*

- 32. Electronic cash (or 'e-cash') seeks to provide a way of paying for goods and services across the Internet. In concept, e-cash would replace notes and coins for normal Internet transactions; however, it has the added advantage of being able to be split into fractions of the lowest denomination coins to allow what are termed 'micropayments'. These small payments could be made for reading specified sections of on-line newspapers, for example. Under most existing payment systems, these micropayment transactions would not be economical. With e-cash, the customer buys value from an authorised provider as with the smart card however, the value is then stored either in customer's home computer or a safe repository on-line. When the funds are spent, the e-cash value is credited to a retailer's e-cash account that then must be later 'up-loaded' to the retailer's regular bank account. Security of e-cash systems is concerned primarily with ensuring that value cannot be created except by authorised institutions or that the same value cannot be spent more than one time.
- 33. Concerns with regard to e-cash are generally the same as those mentioned for smart cards. Since only the initial purchase and the final settlement stages take place through banks, the risk exists that there will be no way to track e-cash in transactions taking place after the initial purchase and before final crediting of the value to a retailer's account. Some systems currently being tested have set limits to the amount that an e-cash 'purse' may hold; however, there is at present no uniform regulatory standard, and it is not certain that such regulations would do much to limit the use of e-cash by the consumer. The anonymity of e-cash, similar to coin and banknotes, may also hinder the financial institution with reporting obligations from positively identifying the ultimate source of an e-cash transaction. A further concern is that currently available computer encryption systems may further shield e-cash transactions from the scrutiny of investigative authorities.

b. Countermeasures

- 34. Smart cards appear to be able to replicate all of the functions of e-cash while allowing portability and use in the real world, as well as over the Internet. There was some uncertainty expressed, therefore, over the ultimate success of e-cash systems. Nevertheless, the experts agreed that the field of new payment technologies is changing very rapidly, and that developments in e-cash systems, along with those of the other proposed systems, should continue to be monitored. The experts discussed a number of possible measures that might limit the vulnerability to money laundering on the new payment technologies. These measures included the following:
- limiting the functions and capacity of smart cards (including maximum value and turnover limits, as well as number of smart cards per customer);
- linking new payment technology to financial institutions and bank accounts;
- requiring standard record keeping procedures for these systems to enable the examination, documentation, and seizure of relevant records by investigating authorities; and
- establishing international standards for these measures.

(iv) Potential use of the gold market in money laundering operations

a. General

- 35. Following last year's introduction to the issue of money laundering through the gold market, the FATF experts were asked to provide specific examples of such cases from their national experience. A number of members did provide example of cases in which gold transactions were an integral aspect of the investigated money laundering scheme. These cases involved the purchase of gold with illegally obtained funds. The gold was then exported to other locations where it was sold, these funds thus being legitimised as the proceeds of gold sales. Existing reporting requirements for gold purchases were circumvented by structuring the purchases to amounts below the reporting threshold.
- 36. Several members reported that the vulnerability to money laundering within their countries has increasingly centred on specialised gold bullion sellers. This is due in part to the fact that anti-money laundering legislation targeting traditional financial institutions has generally caused those customers desiring to purchase bullion anonymously to turn to other sources. In many FATF member countries, there is no suspicious transaction reporting requirement directed toward bullion dealers or other non-financial banking institutions dealing in gold. Additionally, even though the import or export of gold bullion seems to be a key part of money laundering schemes involving the material, members reported that the lack of import / export reporting requirements appears to hamper detection of illegal operations.
- 37. Members were in some cases able to identify cities or regions within their jurisdictions that specialise in legitimate gold business (for example, Cordobá in Spain and Arezzo and Vicenza in Italy) or in which significant business takes place (Paris region and Marseilles in France). Gold purchases in these areas are often conducted in cash and frequently in non-indigenous currency (especially US dollars). Gold serves as both a commodity and, to a lesser extent, a medium of exchange in money laundering conducted between Latin America, the United States and Europe. In this cycle, gold bullion makes its way to Italy via Swiss brokers. There, it is made into jewellery, much of which is then shipped to Latin America. In Latin America, this jewellery (or the raw gold from which it was made) then becomes one of, if not the most important commodities (others include various consumer goods and electronic equipment) in the black market peso exchange money laundering scheme.
- 38. Several FATF members also mentioned having received suspicious transaction reports involving gold transactions. In some instances, these transactions appeared to reflect attempts to avoid high VAT rates by making large purchases of gold in countries with low VAT rates and then exporting the bullion back to the country of origin where it could then be resold at a profit.

b. Hawala / Hundi alternative remittance system and gold

39. The question of laundering through the use of gold as a commodity and as a medium of exchange was discussed by the experts in the context of the hawala / hundi alternative remittance system. The word 'hawala' means 'trust' or 'exchange'; 'hundi' means 'bill of exchange'. It is an alternative remittance system that enables the transfer of funds without their actual physical movement (often without the use of a traditional financial institution). Very often, using hawala is more cost effective and less bureaucratic than moving funds through officially recognised banking systems. Built on a system of trust and close business contacts, hawala originated in South Asia; however, it is now used as an alternate remittance system throughout the world.

- 40. In the laundering associated with this system, gold often plays the role of the primary medium of exchange in certain transactions. Although many hawala transactions may take place without gold, many of these transactions involving the movement of money to South Asia often do involve the metal. There are two reasons for this: the first is the combined historical, religious and cultural importance that gold enjoys in the region, and the second is the increasing distrust in the value of local currencies (many South Asian nations prohibit speculation on their currencies, and exchange rates are fixed by the central banks). Worldwide, gold is often used as a hedge against inflation; in South Asia, gold is often the primary means of preserving and protecting wealth.
- 41. In one scenario, a gold dealer operating in one country also operates as the 'banker' for various jewellery shops in his region. These jewellery shops give him the cheques and cash they receive for purchases; he processes these through his own bank accounts. In return, he furnishes them with scrap gold and gold jewellery for use in their businesses. He retains a few percentage points of the money he receives from them for his 'services' (as well as for the legal risk he is incurring). The owners of the jewellery shops do not have to deal with the bureaucracy of banking, and, since there is almost no paper trail of their sales, they enjoy a greatly reduced tax liability.
- 42. In another scenario, money may be moved from one country to another through the hawala system. A 'hawaladar' (hawala broker) based in one country facilitates this movement by receiving payments in the local currency. He then makes contact with a hawaladar in South Asia and instructs him to make the necessary payment to a specified beneficiary in that local currency. In order to settle his accounts with the South Asian hawaladars, the hawaladar in the first country might send postal money orders or some other financial instruments to a precious metals house in the Persian Gulf. This precious metals house then effects payment to the South Asian hawaladar in gold (either into a safe-keeping account under his name or by direct export of the gold to the South Asian location).

III. MONEY LAUNDERING TRENDS IN FATF COUNTRIES

(i) Sources of illegal funds

- 43. Narcotics trafficking appears still to be the primary single source of criminal proceeds among the majority of FATF members. The various types of fraud (fiscal, EU funds, value added tax, insurance, bankruptcy, etc.) are the next major source of illegal funds, if not, in some jurisdictions, the primary source. Organised crime activity generates a considerable amount of illegal proceeds that are laundered in or through FATF member countries. Some members have noted with concern the increasing trend for these crime groups to operate in loose alliances (Russian and Latin American groups, for example). Written submissions from some of the members also mentioned an increase in the number of cases in which laundering was related to official corruption or the funding of international terrorism.
- 44. The United States has recently substantially elevated the priority assigned to combating terrorist financing (which can constitute the crime of money laundering in the United States). In October 1997, the US government designated 30 foreign organisations as foreign terrorist organisations. In June 1998, US federal authorities seized USD 1.4 million in cash and property held by individuals and an organisation whose funds were reportedly part of a scheme to support Middle Eastern terrorism. The funds were transferred by wire from Europe and the Middle East to financial institutions in the United States and, through various means, were then used to facilitate recruitment, training, and operations of the terrorist group Hamas. This case marks the first time that civil asset forfeiture laws were used in the United States to seize assets suspected of being involved in money laundering violations related to foreign terrorism.

These terrorist operations included a conspiracy to commit extortion, kidnapping, and murder against the citizens and the government of Israel.

- (ii) New or significant trends
- a. General
- 45. Many of the submissions of FATF member countries noted an increase in suspicious transaction reporting, both for certain individual money laundering methods and in overall numbers of reports. As for new methods, however, with the exception of new payment technologies described above, the submissions appear to indicate that launderers are using the same practices that they have done in the past. Money laundering within FATF members is characterised, therefore, by a finite number of techniques that can be combined into an almost infinite variety of laundering schemes. Laundering activity is also characterised by its ability to change quickly when faced with new countermeasures by shifting to other techniques or mechanisms, combining these methods into new schemes, or by moving to sectors or regions where government oversight represents less of a threat.
- 46. Indeed, this last point was cited by virtually all members as a fundamental truth of money laundering today: the lack of comprehensive preventive measures in a particular sector or region will inevitably attract money laundering activity. Members continue to mention bureaux de change, money remittance businesses, and casinos as particularly vulnerable to laundering in some locations. Often these are combined with cash smuggling, alternate remittance systems, or the use of offshore registered businesses, all of which generally operate beyond the framework of traditional financial oversight systems.
- Another particularly evident trend in the money laundering schemes described by the FATF experts is the growing role played by professional services providers. Accountants, solicitors, and company formation agents turn up ever more frequently in anti-money laundering investigations. In establishing and administering the foreign legal entities which conceal money laundering schemes, it is these professionals that increasingly provide the apparent sophistication and extra layer of respectability to some laundering operations. These services are offered not only at offshore locations (as described above) but also within FATF member countries. One delegation described a money laundering scheme in which a criminal group selected a firm of solicitors to act on their behalf in the purchase of a company. The funds for the purchase were delivered to the solicitors in cash and placed in a client account. When the purchase later fell through, the funds were returned — less fees — to the criminal group in form of a cheque. In fact, the group already owned the company they were attempting to 'buy' and had arranged for the failure of the sale since they only wished to convert their criminal proceeds into a cheque from a respectable law firm. This scheme was revealed in a suspicious transaction report from the law firm concerned. More often than not, however, professional services providers are still not subject to suspicious transaction reporting requirements in FATF members. Even when they are subject to such a requirement, the numbers of disclosures made to authorities are frequently disappointing.
- 48. Even in instances where preventive measures have been implemented, laundering activity still occurs, according to the FATF experts. When faced with suspicious transaction reporting at both banks and other financial services, launderers frequently resort to structured transactions to avoid the reporting threshold. Despite border controls designed to detect smuggling of cash criminal proceeds, bulk shipments of cash continue to be observed by FATF members. The use of legitimate appearing business transactions claiming that proceeds are generated by a legal currency exchange business, the profit from bona fide commodity sales, the result of factoring operations, for example is a standard cover used by launderers to hide the criminal origin of those funds. Members mentioned that the only indicator of money laundering

in these cases is often the disproportionate size of the transactions (either individually or in aggregate) when compared to the expected economic activity of the business.

- 49. Several FATF members reported an increase in the appearance of insurance products in laundering schemes. Various products have been noted, including life and property insurance and long term capitalisation bonds. Launderers generally pay for the insurance using the cash criminal proceeds. They then request early pay out of the policy (in the case of life insurance or capitalisation products) or make a claim against the property insurance, thus obtaining a 'legitimate' insurance refund or claim payment.
- 50. Electronic funds transfers continue to be the preferred method for the layering of criminal proceeds once they enter the legitimate financial system. Frequently, these proceeds are smuggled out of the FATF member country, deposited into the financial system at a foreign location, and then wired back to the country of origin. Wire transfers are often associated with foreign registered business entities as described above. If criminal proceeds are transmitted through 'transit' accounts set up in offshore financial centres or as have been found in some FATF member countries according to the written submissions the beneficial owner of the funds is effectively hidden.

b. Derivatives and securities markets

- 51. In recent FATF meetings, questions have arisen concerning the perceived vulnerabilities of the derivatives and security markets as a vehicle for money laundering. As part of the written submission of one member, a paper was prepared on this issue and provided to the experts. According to the paper, there is good reason to suspect that money laundering may pose a substantial threat in these markets. Compared to banks, the derivatives markets and associated products represent perhaps a better opportunity for laundering because of the ease with which audit trails can be obscured. Indeed, any product that offers rapid commercial decision making, high speed transfer, obscurity of control, or complication of audit trail is at risk. Operators in these markets, when compared to banks, tend to be less familiar with anti-money laundering efforts. There is also evidence a good example is the BCCI case which shows the readiness of criminals to use financial products for laundering.
- 52. The primary opportunity for laundering is in the complex derivatives market. Derivatives are securities that derive their value from another underlying financial instrument or asset; they have no intrinsic value of their own. There are three primary types of derivative contracts: forward contracts, futures, and options. All of these instruments, in simple terms, are contracts sold as a hedge against the future risk of fluctuations in commodity prices, time differentials, interest rates, tax rates, foreign exchange rates, etc. Because of the flexible nature of these products, the derivatives market is particularly attractive to operators willing to risk heavy losses. A high volume of activity on the market is essential to ensure the high degree of liquidity for which these markets are known. The way in which derivatives are traded and the number of operators in the market mean that there is the potential obscuring of the connection between each new participant and the original trade. No single link in the series of transactions will likely know the identity of the person beyond the one with whom he is directly dealing.
- 53. The derivatives markets have traditionally not been subject to strict regulatory oversight under the assumption that its operators, as high risk investors, do not need the same level of protection. The introduction of stricter controls would necessarily cause investors to look elsewhere for these markets. For fear of scaring of investors, there is thus no incentive for traders on the market to ask too many questions. This lack of rigorous government control makes the derivatives market even more attractive from the perspective of a money launderer.

- (iii) New countermeasures implemented or significant modifications to existing measures
- 54. The level or type of money laundering activity can change rapidly in response to countermeasures implemented by a particular jurisdiction. FATF members continue to re-examine their anti-money laundering efforts and refine them where necessary. Faced with difficulties in prosecuting money laundering under provisions dealing with receipt of stolen goods, Sweden and the Netherlands plan to set up separate offences of money laundering under their respective penal codes. Some FATF members have extended the list of predicate offences for laundering or plan to do so.
- 55. Several FATF member countries are working to extend preventive measure (suspicious transaction reporting) beyond the traditional banking sector. New Belgian legislation this year, for example, extends suspicious transaction reporting (STR) requirements to real estate agents, bailiffs ('huissiers de justice'), money courier services, notaries, accountants, and casinos. Sweden plans to introduce a reporting requirement on money laundering for external auditors.
- The Netherlands has introduced legislation which requires money transfer businesses to report unusual transactions. Germany has already placed a requirement on such businesses to obtain a licence from the Federal Banking Supervisory Office (FBSO), the same authority that oversees banking activity. Additionally, the FBSO requires that all transactions dealing in foreign currency valued at DEM 5,000 (USD 3,018) require customer identification. Finland has extended suspicious transaction reporting to its entire financial sector, includes casinos and other gambling related businesses, and has consolidated reporting to a single financial intelligence unit. Similarly, Switzerland's reinforced money laundering legislation, which also establishes a centralised reporting unit, came into effect in April 1998. This legislation also extends the suspicious transaction reporting obligation to all financial sectors.
- 57. Japan plans to enact legislation that will strengthen its measures for combating money laundering and organised crime, and this legislation is currently under deliberation in the Diet. This legislation will extend the number of predicate offences for money laundering, provide for enlargement of the measures for confiscation and freezing the proceeds of crime, and centralisation of suspicious transaction reporting under the Financial Supervisory Agency.
- 58. Canada is working to amend existing legislation to require mandatory reporting of suspicious transactions, as well as cross border movement of currencies. The amendment will clarify the ambiguity surrounding the definition of suspicious transactions and when they are required to be reported. Legislation permitting law enforcement to conduct money laundering sting operations has already been implemented.
- 59. It has become clear that the analysis and discussion of trends in virtually all FATF member countries now begins with analysis of suspicious transaction reports. Preventive systems involving these reports, implemented and used widely to help detect individual instances of money laundering, are the starting point for examining the money laundering phenomenon from a more strategic point of view. This is reflective of the increase in the number of FATF member states which now have functioning financial intelligence units (FIUs) and mandatory suspicious transaction reporting regimes. The written submissions of the experts, as well as the discussions during the typologies meeting indicated that suspicious transaction reporting systems are becoming more effective in detecting new money laundering methods. The ability of FIUs to share information, even informally, has also dramatically increased.

IV. MONEY LAUNDERING TRENDS OUTSIDE FATF COUNTRIES

60. Money laundering is a problem that is not restricted to FATF members alone. Countermeasures implemented in FATF member countries have facilitated the collection and analysis of information on money laundering activity within their respective national areas. These countermeasures have also, in some cases, pushed certain money laundering activity to jurisdictions having little or no anti-money laundering regime. At the same time, an increasing number of non-FATF countries have established or are in the process of developing effective money laundering countermeasures. Nevertheless, information provided by the FATF experts on non-member countries is far from complete; therefore, the following assessment of money laundering trends outside the FATF member countries does not claim to be exhaustive.

(i) Asia and the Pacific Region

- 61. Sources of information on money laundering activities in the region have been limited. While few non-FATF members in the area have implemented comprehensive anti-money laundering programmes, there have been some signs that individual countries are moving to establish such systems. Some FATF members nevertheless continue to find evidence of significant money laundering activity or serious vulnerabilities to it.
- 62. As noted in previous typologies exercises, South Asia continues to be one locus in the region for such activity. It serves as home to several major international banks and is a transhipment point for drugs produced in Afghanistan and Iran to the west and in Myanmar, Thailand, and Laos to the east. Money laundering related to the narcotics trade, financial fraud, corruption, and other activities is believed to be carried out through both the traditional banking system and the hawala / hundi alternative remittance system.
- 63. In the Pacific region, a heavy concentration of financial activity related to Russian organised crime has been observed, specifically in Western Samoa, Nauru, Vanuatu, and the Cook Islands. One delegation mentioned an increasingly common scheme whereby apparently American middlemen are used to open accounts or charter banks in one of the locations. Given the increased suspicion aroused by visible Russian business activity in these jurisdictions, the laundering scheme thus operates under the cover of non-Russian linked business. Internet gambling, which generates nearly \$1.5 million a month in this region, represents a major new business trend in Western Samoa, Niue, Vanuatu, Tonga, and Fiji and another potential vulnerability for money laundering and financial crime in those jurisdictions.
- 64. FATF members greatly welcomed the fact that the Asia/Pacific Group (APG), this region's new anti-money laundering body, held its first typologies workshop in October 1998 in Wellington, New Zealand. Experts from 25 jurisdictions in the area and 4 international organisations met for two days to highlight the most significant money laundering issues of their particular jurisdictions, as well as the Asia/Pacific region as a whole. The Asia/Pacific Group had not yet released its final typologies report by the time of the FATF experts meeting; however, the group provided a short submission to the FATF which described some of the key findings of the APG experts.
- 65. The primary sources of criminal proceeds in the region were identified as trafficking in human beings and illicit drugs, gambling and the activities of organised crime groups. Some other identified sources include kidnapping, arms smuggling, hijacking, extortion, public corruption, terrorism and tax evasion. It was also noted that the perpetrators of the predicate offences commonly launder their own proceeds.
- Among some of the methods employed for laundering, the APG experts cited the abuse of offshore financial centres and the increasing presence of solicitors, accountants, and other professionals both to set

up business entities and facilitate the administration of accounts used in money laundering. Structured transactions, purchase of monetary instruments (bank drafts, cheques), and physical removal of currency or monetary instruments were also observed in the region. Criminal proceeds have been moved through the Asia/Pacific area by traditional (electronic) means, as well as alternative remittance systems. The APG experts also mentioned that criminal proceeds are often transferred out of the region under the guise of real estate or other investments, legitimate gambling proceeds, and through the use of credit and debit cards. The group expressed similar concerns to those mentioned by the FATF members regarding the development of new payment technologies.

67. FATF members welcomed the APG decision to hold an annual typologies workshop and noted that the second APG workshop will be held in Tokyo, Japan, on 2-3 March 1999. The workshop will concentrate on the use of underground banking and alternative remittance systems for money laundering purposes.

(ii) <u>Central America, South America, and the Caribbean Basin</u>

- 68. Drug trafficking and the money laundering activity it engenders continue to be major problems in this region. While most of the countries of the Western Hemisphere have moved to enact anti-money laundering legislation, a number of jurisdictions have not fully implemented these countermeasures. Potential alliances between the region's narcotics traffickers and Russian organised crime, already detected by some FATF members, are a cause for concern, as they may further expand money laundering connections with Europe, North America, and the Pacific regions.
- 69. With regard to the Caribbean area, the Caribbean Financial Action Task Force (CFATF) completed the last phases of its typologies exercise. The exercise comprised four parts conducted over a two-year period. As mentioned in last year's report, the first two phases of its exercise examining laundering activities in domestic financial institutions and through the gambling industry took place during 1997. Since then, CFATF has undertaken an assessment of laundering as it occurs in international financial transactions conducted in both domestic and offshore financial institutions, and also the emerging cyberspace technologies. It is most encouraging to see that CFATF will organise a typologies conference on the vulnerabilities of free trade zones to money laundering activity. CFATF plans to use the conference, which will be hosted by Aruba in 1999, to develop a model free zone compliance programme and code of conduct.
- 70. Money laundering activity in the Caribbean region remains a significant problem due to its location near major narcotics production and consumption areas and its concentration of offshore financial centres. Antigua was again cited as particularly vulnerable due to its failure to implement fully its existing antimoney laundering legislation. Free trade zones were also mentioned as continuing targets for money laundering schemes. In one instance, wire transfers have increasingly replaced cash deposits as the means of moving illegal proceeds through the jurisdiction. St. Kitts was mentioned as being of some concern due to a reported increase in narcotics related laundering activity. Suspicious transactions have been detected within French overseas departments in the Caribbean area relating to structured deposits.
- 71. The laundering of criminal proceeds continues to affect the many other nations of Latin America. Narcotics trafficking remains the primary source of these proceeds. Despite steps taken by the Mexican government in the past year to address the problem, laundering activity is still of serious concern in that country. Cross-border laundering of drug proceeds between the United States and Mexico continues with currency smuggling, use of payable through accounts, bureaux de change and the black market peso exchange identified as the key laundering methods. Mexican drug cartels remain the primary force in this activity, although the Colombians still play a role. These organisations are able to operate in Mexico by

taking advantage of loopholes in existing legislation. Corruption continues to hamper the country's antimoney laundering efforts.

- 72. Costa Rica was mentioned in connection to laundering activity through financial institutions, casinos, bureaux de change, bulk currency smuggling, and real estate investments. As reported last year, Colombia continues to see the black market peso exchange being used as the primary money laundering system by narcotics traffickers based in that country. The rising cocaine demand in Europe has reportedly resulted in an increase in funds needing to be laundered in the area and the formation of new alliances between Colombian narcotics traffickers and Russian organised crime groups.
- 73. With its role as a major finance and trading centre and its proximity to Colombia, Panama remains attractive to money laundering schemes. The Colón Free Zone is a key target for these laundering activities despite the extension of anti-money laundering measures to the area. Suriname is another country of the region that has an increasingly visible money laundering problem. Methods detected in that country include over-invoicing, gold purchases and account manipulation. Recently, high-level Surinamese officials have been implicated in laundering activity related to international narcotics trafficking.

(iii) Central and Eastern Europe

- 74. The countries of Central and Eastern Europe remain a significant concern to FATF members. Illegal proceeds are generated by contract and privatisation fraud schemes, as well as from the extraction and production of natural resources. In Central Europe, financial institutions continue to be victims of fraud schemes using misrepresented collateral and carried out with the collusion of bank officials. Embezzlement of corporate funds through false contracts is also still a problem.
- 75. Organised crime activity operating out of the former Soviet Union area was mentioned as being of continuing concern. Many of these organised crime groups bring their criminal proceeds to the nearby FATF members in Europe where they make large real estate investments in such areas as the French and Spanish Mediterranean coast. The groups frequently transfer their funds through various offshore financial centres, such as the Channel Islands, Gibraltar, and the Caribbean area, before using the funds for these investments. The transfers are sometimes made in the name of a legitimate appearing business entity registered in an FATF member country; however, upon further investigation, it is found that the company has no place of business or bank account in the country of registry.
- 76. FATF members also noted their concern over potential connections of financial institutions to Eastern European organised crime. It is difficult to determine the exact role that Russian financial institutions may wittingly or unwittlingly play with regard to organised crime activity. This difficulty extends to Russian business entities, as well. One member noted that banks operating in Europe seem to be less critical when dealing with other banks even if the counterpart is Russian.
- 77. A number of members noted an increase in the number of couriers of Central or Eastern European origin involved in reports of unusual or suspicious transactions. These transactions seem especially prevalent with regard to operations at bureaux de change located in FATF member countries. The couriers have no known business or residence connections in the country where they attempt to conduct single transactions with relatively large amounts of cash (individual transactions range from USD 50,000 to USD 100,000). The large sums and the manner in which the transactions occur seem to indicate that these individuals are not simple tourists.

- 78. Central and Eastern Europe countries have made a certain amount of progress in developing, adopting and implementing countermeasures during past year. Some examples of this progress include the following: Bulgaria, Estonia, Latvia, Lithuania, and Romania have all enacted anti-money legislation. Latvia and Lithuania have operational financial intelligence units, and Poland hopes to have an operational unit in the first part of 1999. Despite its many internal problems, Russia has enacted a new criminal code that includes money laundering as a crime. The Russian anti-money laundering legislation is scheduled to be approved by the country's parliament in early 1999. Ukraine has effectively abolished anonymous accounts, and its Ministry of Justice is in the process of drafting its first comprehensive anti-money laundering laws. Nevertheless, some FATF members noted that it is still often difficult to obtain information relating to anti-money laundering investigations from certain of the countries of the region. One member mentioned that many of the Central and Eastern European countries have experienced similar frustrations in attempting to obtain information on foreign registered business entities from offshore financial centres in support of their anti-money laundering investigations.
- 79. FATF welcomed the further development of the Council of Europe initiative to evaluate anti-money laundering systems. The select committee set up for this purpose has adopted an evaluation process based on the one used by the FATF. Its goal is to evaluate the countermeasures in place in each of the 21 members of the committee (the non-FATF members of the Council of Europe). During the past year, the committee conducted seven mutual evaluations. The committee also held its first typologies exercise in December 1998, and it is hoped that this will become a recurring event. Indeed, the Council of Europe typologies exercise, along with those of APG, CFATF, and the FATF, should become the basis for a much clearer picture of money laundering activities throughout the world.

(iv) Middle East and Africa

- 80. Information on laundering activities in this area of the world is extremely limited. A number of factors favourable to money laundering are known to be present throughout both regions. In the Gulf States (particularly in Bahrain), the banking and finance industries are well established on an international scale. Only a few of the jurisdictions of the region have anti-money laundering legislation. Many expatriate labourers working in the region regularly send money home by using the traditional hawala / hundi alternate remittance system, which offers more favourable rates than those of traditional banks. Gold smuggling is also reportedly used especially by some professional criminal organisations as a means of moving funds through the Gulf into the South Asian region. Free trade zones of the area are also likely to attract some of this laundering activity.
- 81. Still less is known about the Mediterranean area. The growing presence of its own financial centres and its role as a drug transit area appear to make the region vulnerable to laundering activity. Such activity involving organised crime and the diamond industry in Israel has been observed by some FATF experts. With only a few exceptions, most jurisdictions of the region are characterised by the total absence of comprehensive anti-money laundering programmes.
- 82. Africa south of the Sahara is also considered by many of the FATF experts to be vulnerable to money laundering, although, again, information on the region is limited. A factor which contribute to this vulnerability is the increasingly widespread activity of indigenous and, to certain extent, non-indigenous organised crime groups. These groups can operate throughout the region due to lack of strong anti-money laundering laws, combined with the endemic corruption, lack of training, and low pay of government authorities. Only South Africa has criminalised money laundering for crimes beyond those related to narcotics trafficking; however, it has yet to enact comprehensive preventive measures. In other countries of

the region, it is believed that only about 20% of the population use traditional banks; thus, there is some concern about how preventive measures could be applied there.

83. FATF experts noted again the ubiquity of West African (especially Nigerian) organised crime groups in money laundering schemes that link FATF countries with the region. As noted in previous reports, fraud seems to be one of the most pervasive sources for laundered funds; however, these groups are also involved in narcotics trafficking, arms smuggling, auto theft, gemstone and ivory smuggling, and trafficking in stolen identity documents. One member noted that there were increasingly ties with some of the francophone countries of western Africa, particularly Togo, Benin, and Senegal. In general, there appears to be a growing frequency of using bureaux de change operations as a cover for converting criminal proceeds. Some groups are using bank accounts in FATF member countries as collector accounts for these proceeds. Funds from these accounts are then used for the purchase of goods that are shipped to Africa and sold as 'legitimate' imports. The holders of these accounts charge a percentage for their use but otherwise have neither interest in the source of the funds nor any direct link to the transactions.

V. CONCLUSIONS

- 84. The London meeting of the group of experts on typologies in November 1998 was the second to undertake in-depth discussions on more focused topics. As mentioned last year and as evidenced by the written submissions of the FATF delegations, the basic techniques and mechanisms for money laundering have been well documented. This meeting examined a number of areas that had not been fully developed. It is hoped, therefore, that the purpose of these expert meetings will continue to be the identification of new approaches taken by launderers, along with significant changes in the patterns of their activity. Through this work, the FATF will acquire additional support and, one might hope, new ideas for appropriate laundering countermeasures.
- 85. With regard to the money laundering implications of the introduction of the euro in the eleven members of the Economic Monetary Union, experts agreed that there was a potential risk of overwhelming of existing preventive measures due to the increased burden of work for financial institution personnel during the transition phase. The experts also agreed that the introduction of the euro would be a possible opportunity to detect laundering activity. The critical time as far as risk is concerned is the period from January to June 2002, when euros in coin and paper form will replace national currencies. Existing preventive countermeasures should be adequate in detecting possible laundering activity, although a number of FATF members are taking extra steps to re-emphasise or reinforce their anti-money laundering programmes. Some experts believe that the introduction of the large denomination euro banknote (EUR 500) after 1 January 2002 could affect laundering activity by reducing the bulkiness of criminal proceeds when transported.
- 86. Non-cooperative jurisdictions or territories remain a continuing area of concern to FATF members. The inability to obtain relevant information on the beneficial owners of foreign legal entities shell companies, international business corporations, offshore trusts, etc. represents one of the major roadblocks to successfully detecting, investigating and prosecuting suspected international money launderers. There is the need to foster increased awareness of this problem and exert pressure on certain offshore financial centres in international fora where appropriate. The efforts of the FATF ad hoc working group on non-cooperative countries both FATF and non-FATF members will be most welcome in this area.

- 87. Rapid development and growing consumer acceptance of smartcards, on-line banking, and e-cash continue to be the hallmark of these new payment technologies. As recently as two years ago, many of these systems were not yet beyond the prototype stage, and the potential implications on laundering activity were seen as theoretical. Smartcards are beginning to move beyond testing, and on-line banking is already a reality in a few FATF member countries (and potentially available world-wide through the Internet). The abuse of these systems by launderers is no longer a distant possibility. FATF experts noted that certain money laundering countermeasures could be easily added to the systems; however, decisions to do so have been left to the system developers. Without consistent standards and appropriate regulatory oversight, these new payment technologies will remain highly vulnerable to money laundering activity.
- 88. Awareness of the potential role of the gold market and, by extension, of other high-value commodities markets is growing among FATF member countries. Transactions involving gold are increasingly found in money laundering schemes and are often an integral part of money movements through various parallel banking systems, such as the hawala / hundi system discussed during this typologies meeting. It was emphasised that these money laundering schemes are not limited to any single region of the world. Nevertheless, the particular focal point of gold dealers in the Gulf States for hawala / hundi money movements to and from the South Asia region should be noted.
- 89. The experts noted the apparent increasing trend for professional services providers accountants, solicitors, company formation agents, and other similar professions to be associated with more complex laundering operations. These professionals set up and often run the legal entities that lend the high degree of sophistication and additional layers of respectability to such money laundering schemes. Operating not only in certain offshore locations where they are protected behind a wall of strict confidentiality, these professionals sometimes also provide similar services within FATF member countries themselves. Currently, only a few FATF members impose an obligation on professional services providers to report suspicious transactions. Those members that do have this requirement are not always satisfied with the amount of reporting that takes place from this sector, although the quality of individual reports in some cases appears to justify the need for such reporting.
- 90. Lastly, this meeting of experts on money laundering typologies has shown in another way the utility of the preventive measures put in place to counter money laundering. The analysis and discussion of methods and trends in virtually all FATF member countries began with analysis of suspicious transaction reports. These systems, implemented to help detect individual instances of money laundering have now become the starting point for examining the phenomenon from a more strategic point of view. Given the insight that this source of information provides to the state of money laundering in a particular jurisdiction, this use of STRs is an encouraging development.

10 February 1999

ANNEX TO THE 1998-1999 FATF REPORT ON MONEY LAUNDERING TYPOLOGIES

Selected cases of money laundering

Case Nº 1: Accounting firm

Case Nº 2: Structuring scheme

Case Nº 3: Gold smuggling

Case Nº 4: Insurance policies and real estate

Case Nº 5: Front companies

Case Nº 6: Money transfers

Case Nº 7: Offshore financial centres, solicitors, and other financial services providers

Case Nº 8: Front companies, insurance, and bureaux de change

Case Nº 9: The derivatives market: a typology

Case Nº 1

Accounting firm

Facts

Beginning in May 1994, two alleged narcotics traffickers used an accounting firm to launder criminal proceeds generated from amphetamine sales. The 'clients' of the firm would on a regular basis hand their accountant cash in brown envelopes or shoe boxes for which no receipt was issued. The funds were then stored in the accountant's office until he decided how they could be introduced into the financial system and laundered. At any one time, there were between USD 38,000 and USD 63,000 stored in the accountant's office.

The law enforcement agency investigating the matter found that the accountant established company and trust accounts on behalf of his clients and opened personal bank accounts in the names of relatives. He then made structured deposits to those accounts with the funds received from the alleged traffickers. Additionally, he transferred approximately USD 114,000 overseas — again, using structured transactions — to purchase truck parts, which were later brought back into the country and sold at a profit, and also used some of the funds to purchase properties. The accountant and three of his colleagues (who were also implicated in the scheme) reportedly laundered approximately USD 633,900 and received a 10% commission for his services.

Results

The accountant and his colleagues are believed to have acted from the beginning with the suspicion that the clients were involved in illegal activities. Even after obtaining further specific knowledge of his clients' involvement in narcotics trafficking, he and his associates allegedly continued to facilitate money laundering.

Lessons

This case highlights the key role that financial experts can play in the laundering of criminal proceeds. Many of the services provided (establishment of specialised accounts or business entities, making real estate investments) are potential money laundering mechanisms that may be beyond the abilities of the less sophisticated criminal.

Case Nº 2

Structuring scheme

Facts

This case came to the attention of the police through an informant. An individual residing in a small town deposited the equivalent of USD 1,038,354 over a three year period into three financial institutions. The institutions involved were two of the country's major banks and a credit union. Nearly 95% of the deposits were made in cash. The account holder into whose accounts the deposits were made was the citizen of a neighbouring country where there had been an outstanding arrest warrant against him since 1982.

During the investigation, it was determined that the employees of the financial institutions had been suspicious of the account activity. They had noticed, for example, that some deposits were made in brown paper bags through the night deposit drawer, yet they did not disclose this information to authorities. Funds deposited into the accounts were ultimately transferred to the account holder by his writing cheques on these accounts.

Results

Whether or not suspicious transactions were reported was unfortunately left to the discretion of the financial institution. In this case, the institution employees could not be found to have violated any rules. Due to a lack of vigilance on the part of financial institution employees, even to very obvious suspicious financial activity, an individual was able to launder a substantial sum of money.

Lessons

This example reinforces the need to ensure that financial institution employees know what sort of financial activities might be suspicious and thus worthy of reporting. This case illustrates the advantage of mandatory suspicious transaction reporting. Having such an obligation provides an additional incentive for

financial institutions to ensure that their employees have thorough knowledge of what constitutes suspicious financial activity. Furthermore, once in place, mandatory suspicious transaction reporting serves as a deterrent for some of the relatively unsophisticated laundering schemes as described here.

Case Nº 3

Gold smuggling

Facts

In 1997, a financial intelligence unit (FIU) in country A received various suspicious transaction reports involving nationals from Scandinavian countries. These individuals were making large purchases of gold in their own names using cash in the currencies of their home countries. The transactions were conducted at various financial institutions in country A.

Initial examination of the disclosures indicated that the Scandinavian nationals had neither an official address nor any known legal activity in country A. Information obtained from police and FIUs in their countries of origin revealed that some of the participants in the scheme had outstanding arrest warrants for serious tax fraud. The individuals were suspected to have purchased gold in country A and elsewhere (where the value added tax rate on gold is lower). They then sold the gold in their home countries via various companies.

The suspicious transactions initially appeared to be separate incidents; however, they were grouped together based on such factors as profile of the participants, financial organisations target, and the dates of the transactions. At one of the bureaux de change where the transactions took place, examination of numerical sequence of exchange statements and gold sales invoices provided further information on the methods used by the Scandinavian nationals. For example, the suspects would sometimes conduct their transactions together, and at other times they split up their funds and conducted identical operations on the same day with a series of targeted financial institutions. The co-ordination among seemingly separate transactions seems to indicate that participants in the scheme were all likely couriers for the same organisation.

Results

Given the suspicious nature of this group transactions, the dossier was passed over to the public prosecutor in country A. The dossier also contributed useful evidence to ongoing investigations on the home countries of the suspects.

Lessons

Criminal organisations that are willing to devote the human resources to spreading their laundering operation over a larger geographic area are thus more likely to go undetected. This scheme would not have been detected if the various suspicious transaction reports could not have been brought together and compared. Likewise, the full picture of the scheme could not have been developed had there not been information sharing with foreign counterpart authorities.

Case Nº 4

Insurance polices and real estate

Facts

An insurance company informed an FIU that it had underwritten two life insurance policies with a total value of USD 268,000 in the name of two European nationals. Payment was made by a cheque drawn on the accounts of a brokerage firm in a major EU financial market and a notary in the south-eastern region of the country.

The two policies were then put up as collateral for a mortgage valued at USD 1,783,000 that was provided by a company specialising in leasing transactions. As the policyholders did not pay in their own name, the issuer contacted the brokerage firm in order to discover the exact origin of the funds deposited in its account. It was informed that the funds had been received in cash and that the parties concerned were merely occasional clients.

The parties — two brothers — were known to a law enforcement agency through a separate investigation into the illegal import and export of classic automobiles. Moreover, two individuals with the same surname were suspected by the same agency of drug trafficking and money laundering.

Results

This case has not yet been passed to the prosecutorial authorities.

Lessons

This example shows the necessity for non-bank financial businesses (in this case insurance companies) to be aware of what constitutes suspicious financial activity. It also demonstrates the critical need for effective co-ordination between the information contained in suspicious transaction reports and law enforcement information.

Case Nº 5

Front companies

Facts

An FIU in country B received a report of a series of suspicious transactions involving the bank accounts of a West African citizen and his businesses, which specialised in industrial fishing. These accounts were opened in banks located in country B and consisted primarily of money changing operations. The businessman also owned several residences in his home country and in the capital region of country B. The companies that he jointly managed all had the same address in his home country.

The personal account of the West African businessman received a number of transfers from accounts in another European country and in his home country (over USD 2 million from 1995 to 1996). The business accounts of the companies received transfers from several business entities based in Europe which were ostensibly linked to fishing related activities (over USD 7 million from 1994 to 1997). The transfers out of the account (estimated at nearly USD 4 million over the same period) were made to various companies

whose business was (according to official records) connected with maritime activity and to other individuals.

The FIU's analysis showed that the income of the West African companies concerned was grossly disproportionate to reported sales. In fact, the account transactions seemed to have little to do with industrial fishing (i.e., foreign currency sales, transfers from the bank accounts of European residents, transfers between the personal account of the West African businessman and his businesses, transfers between these businesses and those of Europe-based partners).

Furthermore, according to additional information received by the FIU, one of the partners of the West African businessman, a co-manager of one of the companies, was suspected of being involved in several financial offences in Italy. This individual reportedly had close associations with two Italian organised crime figures, and his Italian businesses have become the target of investigation into money laundering in that country. Still another business partner of the West African businessman appears also to be involved in financial and fiscal offences.

Results

This case has not yet been passed to prosecutorial authorities.

Lessons

Given the unusual account transactions and the lack of a clear economic connections for some of the business activities, the operations described in this example very likely constitute a money laundering scheme to conceal the illegal sources of proceeds derived from various criminal activities. This case gives further support to the need for analysis of information from a variety of sources (suspicious transaction reports, financial institutions, company registries, police records, etc.) in order to gain a full picture of a complex laundering scheme.

Case Nº 6

Money transfers

Facts

In July 1997, the police arrested the leader of an Iranian drug trafficking group, suspect A, for possessing stimulants and other kinds of drugs. The subsequent investigation revealed that the suspect had remitted part of his illegal proceeds abroad.

A total of USD 450,000 was remitted via three banks to an account on behalf of suspect A's older brother B at the head office of an international bank in Dubai. Transfers were made on five occasions during the two months between April and June 1998 in amounts ranging from USD 50,000 to USD 150,000).

Another individual, suspect C, actually remitted the funds and later returned to Iran. On each occasion, C took the funds in cash to the bank, exchanged them for dollars, and then had the funds transferred. Each of the transactions took about one hour to conduct, and the stated purpose for the remittances was to cover 'living expenses'.

Results

Suspect A was initially charged with violating provisions of the anti-narcotics trafficking law. The money transfers revealed during the investigation led to additional charges under the anti-money laundering law. This was the first time that anti-money laundering provisions had been applied to the overseas transfers criminal proceeds. Court proceedings for this case are on-going.

Lessons

This case represents a classic example of a simple money laundering scheme and is also a good example of a case derived not just from suspicious transaction reporting but also as a follow-up to traditional investigative activity.

Case Nº 7

Offshore financial centres, solicitors, and other financial services providers

Facts

In December 1997, M-Bank, acting as an international clearing bank, received a wire transfer for USD 1.4 million that appeared to originate from a UK law firm. The transfer was to be credited to the account of 'AZ Brokerage International, Ltd.' in G-Bank.

Due to the initials used in the company's name, M-Bank suspected that AZ Brokerage International, Ltd. might be a controlled by Mr. 'AZ', who was known to be involved in dubious financial activities. The bank also knew that Mr. AZ had served two years in a foreign prison for his connections to a false monetary instrument scheme and that his personal assets were subject to bankruptcy proceedings.

M-Bank decided to make a suspicious transaction report to the FIU, and, at the same time, they informed G-Bank of their suspicion. G-Bank subsequently disclosed to the FIU that Mr. AZ was operating a number of accounts opened under the names of various companies, including AZ Brokerage International, Ltd.

Preliminary inquiries made by the FIU revealed, among other things, the following:

- A third financial institution, D-Bank, had submitted a report to the FIU a few weeks earlier. The report stated that D-Bank had concluded its banking relationship with Mr. AZ after having received several 'suspicious approaches' from him and from foreign sources.
- Mr. AZ appeared to be the principal of 20 legal entities registered in the national company registry. All of these business entities operated from his home address.
- The names of the businesses indicated involvement in various types of financial activity, such as 'AZ Fiduciary & Nominees', 'AZ Investment & Finance', 'AZ Insurance Guaranty Fund', etc.

- The holding company, AZ Holding, Ltd. was stated to have a fully paid share capital of 20 million USD confirmed by the company's state authorised accountant.
- None of the companies were licensed to provide any type of financial or brokering services in the country of registry, according to the financial supervisory authority.

The FIU requested that the banks disclose additional information on their banking relationship with Mr. AZ or legal entities controlled by him. G-Bank was further requested to freeze the amount of 1.4 million USD as soon as it was credited to the account controlled by Mr. AZ. This additional information revealed that a number of deposits had been made to the relevant accounts prior to the FIU disclosures. All deposits were made by international wire transfer, and the largest amounted to USD 1.5 million. Most of the funds received had been immediately used to purchase bank drafts that were sent to individuals and companies in the United Kingdom and the United States. It was also noted that the purpose of one wire transfer to a US law firm was stated as being a 'legal fee for establishment of AZ Merchant Bank'.

The above mentioned information was submitted to a criminal investigation team, and the next day Mr. AZ requested that G-Bank transfer several hundred US dollars to an offshore bank account in the name of an individual. The transaction was stopped, and Mr. AZ was arrested as he was due to depart on holiday to the Caribbean where he had planned to meet with several apparently associated individuals.

Documents subsequently seized provided the following information:

- The stated share capital of AZ Holding, Ltd. was based on a Certificate of Deposit with the face value of USD 20 million and issued by a Panamanian financial institution.
- Mr. AZ, in addition to the business entities registered in his country, also held beneficial and formal positions in a number of business entities incorporated in several offshore jurisdictions, including 'AZ Private Bank, Ltd.' registered in Antigua.
- The name of the above mentioned 'AZ Merchant Bank, Inc.' had been changed to 'AZ Banque de Commerce, Inc.' on the advice of the solicitor that later arranged for US incorporation.
- Mr. AZ claims to provide various types of financial services, including private banking and issue of 'proof of funds' for use in various types of high-yield investment programmes, etc.
- A large number of foreign clients mainly from Eastern Europe and the United States had made the initial payment in amounts between USD 5,000 and USD 50,000 to get access to his services.

After the arrest of Mr. AZ, the investigation team was contacted and later visited by several individuals who claim to represent the beneficiaries of three of the deposits amounting to nearly USD 3.5 million—including USD 1.6 million that had been frozen. However, no beneficial party was prepared to make a formal statement or to provide documentary evidence of the source of the funds. No formal claims for the release of the seized funds had been received eleven months after the investigation began.

Results

Mr. AZ was released from custody during the on-going investigation. It appeared, however, that he immediately resumed the same business upon his release. The investigative authority has recently requested the assistance of foreign law enforcement authorities in their investigation regarding USD 20 million that had been transferred from an offshore financial centre to the account of one of Mr. AZ's companies.

Lessons

This case illustrates how financial services providers operating in one country or through an offshore financial centre may facilitate money laundering, as well as legitimate business transactions. With any one jurisdiction having only one part of the picture, it is difficult to determine exactly how the whole scheme works. The fact that, after blocking the transfer of funds for eleven months, there were still no concrete claims from the beneficial owners for their return is also a further indication that the funds may not have been of strictly legal origin. This case is also a good example of how financial institutions can work with each other and anti-money laundering authorities to pull together a picture of the suspected laundering scheme.

Case Nº 8

Front companies, insurance, and bureaux de change

Facts

An FIU received a suspicious transaction report from an insurance company that specialised in life insurance. The report referred to Mr. H, born and resident in a Latin American country, as having recently taken out 'two sole premium life insurance policies for a total amount of USD 702,800'. Subsequent information provided to the FIU indicated that the policies premiums had been paid with two personal cheques made out by a third party and drawn against a major bank. The third party, Mr. K, was also a resident in the same Latin American country although not a national of that country. Further checks at Mr. K's bank revealed that both he and Mr. H had signature authority on two business accounts, Sam, Ltd. and Dim, Ltd.

Examination of the accounts showed, especially in Mr K's account, that transactions were carried out on behalf of Mr H. Thus, the account had received funds from abroad and had also been used for other financial products besides the life insurance policies. Indeed, ten cheques in US dollars drawn against American banks and issued by two bureaux de change operating out of the Latin American country where the two men resided, had been deposited into Mr K's account. The value of these cheques totalled USD 1,054,200.

This activity appeared to show that the funds had been used to pay the insurance premium on Mr. H's life and to acquire stakes in investment funds, also for Mr. H, amounting to another USD 210,840. There were also other related transactions in the accounts of the two companies and Mr H's personal account. Cash or cheque transactions for amounts between USD 14,000 and USD 70,000 were among the related transactions. In one instance, a cheque was drawn of the Sam, Ltd. account for USD 63,300 on the day following the deposit of USD 70,280 in cheques into Mr K's account.

Checks into the backgrounds of Mr. H and Mr. K revealed that Mr. H was suspected of being involved in cocaine trafficking in Latin America. Mr. K had some minor violations (writing bad cheques, etc.);

however, he had no serious criminal background. The business activities and backgrounds of Sam, Ltd. and Dim, Ltd. were also looked at. In both instances, the companies had been incorporated with a stock capital of USD 36,400 in which Mr. H and Mr. K had a 50% interest and were joint directors. Queries made at the 'Balance of Payments Office' as to foreign collection and payment revealed a total absence of operations in the previous two financial years.

Result

It appeared, therefore, that Mr. K was being used as the front man for Mr. H's efforts to move funds out of his country of residence. For greater security of the scheme, firms under their control were established that did not perform any corporate or commercial activity. Mr. H received the funds deposited in Mr. K's account through the sole premium insurance policies and shares in investment funds that had been paid for by that account, as well as through indirect income from the companies mentioned. In this case, the FIU believed there to be sufficient signs of money laundering and therefore passed the matter on to prosecutorial authorities.

Lessons

This operation is interesting because it shows that payment instruments or third party involvement having no apparent economic relationship to the transaction are often a key indicator of suspicious activity. It is worth noting that Mr. K was obviously selected based on his lack of prior criminal record and his nationality so as to minimise suspicion. The activities of the front companies were also conducted in such a way as to give the appearance of transactions from corporate activities. The case also highlights the potential value of suspicious transaction reporting by insurance companies.

Case Nº 9

The derivatives market: a typology

The following typology is provided as an example of how funds could be laundered using the derivatives market.

In this method, the broker must be willing to allocate genuinely losing trades to the account in which criminal proceeds are deposited. Instead of relying on misleading or false documentation, the broker uses the genuine loss making documentation to be allocated to the detriment of the dirty money account holder. As an example, a broker uses two accounts, one called 'A' into which the client regularly deposits money which needs laundering, and one called 'B' which is intended to receive the laundered funds. The broker enters the trading market and 'goes long' (purchases) 100 derivative contracts of a commodity, trading at an offer price of \$85.02, with a 'tick' size of \$25. At the same time he 'goes short' (sells) 100 contracts of the same commodity at the bid price of \$85.00. At that moment, he has two legitimate contracts which have been cleared through the floor of the exchange.

Later in the trading day, the contract price has altered to \$84.72 bid and \$84.74 offered. The broker returns to the market, closing both open positions at the prevailing prices. Now, the broker, in his own books assigns the original purchase at \$85.02 and the subsequent sale at \$84.72 to account A. The percentage difference between the two prices is 30 points or ticks (the difference between \$84.72 and \$85.02). To calculate the loss on this contract, the tick size which is \$25 is multiplied by the number of contracts, 100, multiplied by the price movement, 30. Thus: $$25 \times 100 \times 30 = $75,000$ (loss).

The other trades are allocated to the B account, which following the same calculation theory of tick size multiplied by the number of contracts multiplied by the price movement results in a profit as follows: $$25 \times 100 \times 26 = $65,000$ (profit). The account containing the money to be laundered has just paid out \$75,000 for the privilege of receiving a profit of \$65,000 on the other side. In other words, the launderer has paid \$10,000 for the privilege of successfully laundering \$75,000. Such a sum is well within the amount of premium which professional launderers are prepared to pay for the privilege of cleaning up such money. As a transaction, it is perfectly lawful from the point of view of the broker. He has not taken the risk of creating false documentation, which could conceivably be discovered, and everything has been done in full sight of the market.